PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-276188
(43)Date of publication of application : 30.09.1994

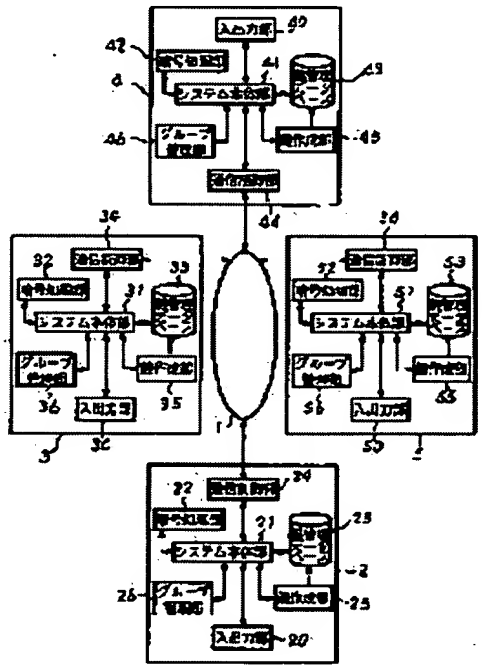
(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
G06F 13/00
H04L 9/06
H04L 9/14
H04L 12/22

(21)Application number : 05-060794
(22)Date of filing : 22.03.1993

(71)Applicant : TOSHIBA CORP
(72)Inventor : OTA TETSUO

(54) ELECTRONIC COMMUNICATION EQUIPMENT

(57)Abstract:
PURPOSE: To improve a processing speed and safety at the time of performing security holding communication by providing a cipher processing part for performing an enciphering processing and a deciphering processing for executing the instruction of a system main body part and a key preparation part for preparing a common key.
CONSTITUTION: This electronic communication equipment connects plural computer systems 2-5 through a communication medium 1. In the electronic communication equipment operated on the computer network, the system main body parts 21, 31, 41 and 51 instruct the mutual identification of users, the distribution of the common key and the transmission/reception of communication information using the common key. Also, the cipher processing parts 22, 32, 42 and 52 for performing the enciphering processing and the deciphering processing for mutually identifying the users, distributing the common key and transmitting/receiving the communication information using the common key and the key preparation parts 25, 35, 45 and 55 for preparing the common key are provided. Thus, it is guaranteed that the communication information is originated from the correct user, the communication information can be deciphered only by the correct user and efficient mutual identification and safe communication can be performed. Thus, the processing speed and the safety at the time of the security holding communication can be improved.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－276188

(43)公開日　平成６年(1994)９月30日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/00					
	9/10					
	9/12					
			8949－5K	Ｈ０４Ｌ	9/ 00	Ｚ
			8949－5K		9/ 02	Ｚ

審査請求　未請求　請求項の数３　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平5－60794

(22)出願日　平成５年(1993)３月22日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　太田　哲生
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内

(74)代理人　弁理士　則近　憲佑

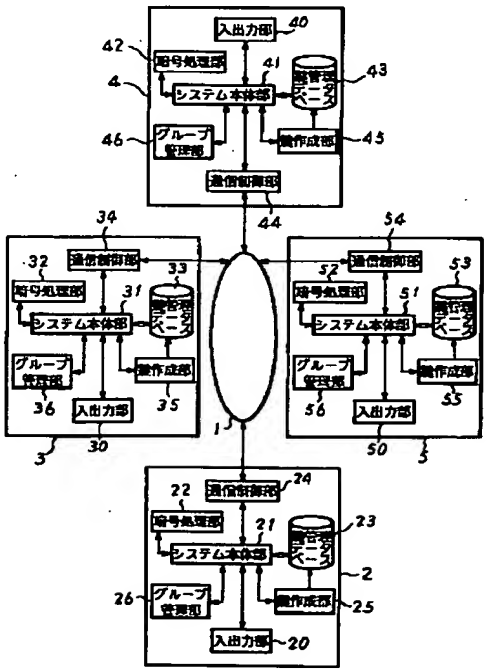
(54)【発明の名称】　電子通信装置

(57)【要約】

【目的】　機密保持通信を行う際の、処理速度と安全性の向上を目的とする。

【構成】　本発明は、コンピュータネットワーク上で動作する電子通信装置において、利用者相互の認証、共通鍵の配布、前記共通鍵を用い通信情報の送受信を命令するシステム本体部と、利用者相互の認証、共通鍵の配布、前記共通鍵を用い通信情報の送受信を行うために暗号化処理と復号化処理を行う暗号処理部と、前記共通鍵を作成する鍵作成部とを具備する。

【効果】　通信情報が正しい利用者から発信されたことを保証し、同通信情報が正しい利用者のみに解読でき、効率のよい相互認証と安全な通信が可能になる。



1

【 特許請求の範囲】
【 請求項1 】複数のコンピュータシステムが通信媒体により相互に接続されたコンピュータネットワーク間で暗号化した通信情報の送受信を行う電子通信装置において、
（ａ）公開鍵暗号方式を用い利用者相互の認証
（ｂ）公開鍵暗号方式を用い共通鍵の配布
（ｃ）前記共通鍵を用い通信情報の送受信
を命令するシステム本体部と、
前記システム本体部の命令を実行するための暗号化処理と復号化処理を行う暗号処理部と、
前記共通鍵を作成する鍵作成部とを具備する電子通信装置。
【 請求項2 】一定時間及び一定通信回数ごとに利用者の一部が前記共通鍵を更新することのできる鍵作成トークンを持つ前記鍵作成部と、
前記利用者の一部が通信を中止するとき、他の利用者に鍵作成トークンの使用を命令するシステム本体部とを具備する請求項1 記載の電子通信装置。
【 請求項3 】サブグループ間の機密保持通信を行うために、サブグループ間に有効な共通鍵を作成する前記鍵作成部を具備する請求項1 記載の電子通信装置。
【 発明の詳細な説明】
【０００１】
【 産業上の利用分野】本発明は、複数のコンピュータシステムが通信媒体により相互に接続されたコンピュータネットワーク上で、機密を保持する機能をもつ電子通信装置に関する。
【０００２】
【 従来の技術】機密保持を行う通信は、通信以前にコンピュータシステムを使用する利用者が正しい利用者であるかを確認すること（ 以下、認証と呼ぶ。）がまず重要である。
【０００３】従来、通常の秘密保持通信と通常の秘密通信通信を行う前の認証を考慮した通信装置として、以下に示す慣用暗号方式を用いた第1 の電子通信装置と第2 の電子通信装置と、公開鍵暗号方式を用いた第3 の電子通信装置があった。
【０００４】慣用暗号方式による２つの電子通信装置は、以下に示す2 つの暗号化の方法の組み合わせによって構成される。第1 の暗号化の方法は、あらかじめ通信情報の暗号化と暗号化された通信情報の復号を行うための一つの鍵を作成し、この鍵をそれぞれ利用者のコンピュータシステムに配布し、配布されたこの鍵を持つ利用者のコンピュータシステムのみ通信可能とする暗号化の方法である。
【０００５】第2 の暗号化の方法は、それぞれの利用者のコンピュータシステムが通信する特定のコンピュータシステム間にのみ有効な鍵を持ち、通信相手ごとに異なるこの鍵を用いて、受信人毎に異なる暗号化した情報を

2

作成し通信を行うための暗号化の方法である。
【０００６】この第2 の暗号化の方法でn 人の利用者が暗号化通信する場合、鍵は全部でn（ｎ－1）／2 個必要であった。例えば、利用者αと利用者βが通信するときの鍵を［ α： β］とする。（ここで、［ α： β］と［ β： α］は同じ鍵であるとする。）５人の利用者α、利用者β、利用者γ、利用者δ、利用者εが通信するとき、鍵は全部で［ α： β］、［ α： γ］、［ α： δ］、［ α： ε］、［ β： γ］、［ β： δ］、［ β： ε］、［ γ： δ］、［ γ： ε］、［ δ： ε］と１０個必要であった。
【０００７】従来の慣用暗号方式を用いた第1 の電子通信装置は、利用者同士の認証と他のコンピュータシステム利用者への通信情報の送信を上述の慣用暗号方式の第2 の暗号化の方法で暗号化通信を行うことを特徴とした装置であり、第2 の電子通信装置は、利用者同士の認証を慣用暗号方式の第2 の暗号化の方法で行い、他のコンピュータシステム利用者への通信情報の送信を慣用暗号方式の第1 の暗号化の方法で行うことを特徴とした装置であった。
【０００８】公開暗号方式を用いた第3 の電子通信装置について以下、「 利用者αが利用者βに情報を送信し、利用者βが利用者αからのこの情報を受信する」という通信を例に説明する。
【０００９】利用者は、それぞれ自分のみが持つ秘密鍵と自分以外の利用者の公開された公開鍵を持つ。この秘密鍵と公開鍵は、（ イ）利用者αの公開鍵で暗号化された情報は、利用者αの秘密鍵で復号する、（ ロ）利用者αの秘密鍵で暗号化された情報は、利用者αの公開鍵で復号する、という対応関係をもっている。
【００１０】この対応関係を利用して、利用者αのコンピュータシステムは、利用者βの公開鍵で情報を暗号化し、さらにこの利用者βの公開鍵で暗号化した情報を、利用者αの秘密鍵で暗号化し送信する。
【００１１】利用者βのコンピュータシステムは、受信した情報を利用者αの公開鍵で復号し、さらにこの利用者αの公開鍵で復号した情報を利用者βの秘密鍵で復号する。
【００１２】このような手順で、情報をやりとりする方法が公開暗号方式を用いた電子通信装置である。これを以下第3 の電子通信装置と呼ぶ。この公開暗号方式を用いた電子通信装置は、ｎ人の利用者が通信するためには自分の秘密鍵と自分以外の利用者の公開鍵を用い、電子通信装置全体で2 ｎ個の鍵を用いる。
【００１３】
【 発明が解決しようとする課題】上述したような第1 の電子通信装置で認証と通信する場合および第2 の電子通信装置で認証する場合は、ｎ人の利用者の認証をする場合、装置全体でn（ｎ－1）／2 個という大量の鍵が必要で、鍵の配布だけでも時間がかかり、また、鍵を記憶

3

させるだけで多くの記憶領域や作業領域を使用してしまい、高速で効率のよい通信が不可能であるという問題点があった。更に、鍵の漏洩については特に対策がなされておらず、通信情報の安全性についての問題点と、１つの情報の送信を行う利用者がn（ｎ－１）／2個の鍵を用いて受信者ごとに送信する通信情報が異なるためネットワーク上の同報機能が使用できず、個別に送信しなければならないという問題点があった。

【００１４】第2の電子通信装置で通信する場合、通信情報の暗号化と暗号化された通信情報の復号を行うための一つの鍵を使用するが、この装置も鍵が漏洩してしまうと機密を保持した通信が不可能であると言う問題点があった。

【００１５】第3の電子通信装置は、１つの情報の送信を行う利用者がそれぞれの受信者の公開鍵を用いて受信者の数だけ暗号化通信を行う必要があるため、時間がかかり、受信者ごとに送信する通信情報の内容が異なるためネットワーク上の同報機能が使用できず、個別に送信しなければならないという問題点があった。また、長時間同一の鍵を使用する場合、鍵の漏洩の可能性もあり、通信情報の安全性についても問題点があった。

【００１６】

【課題を解決するための手段】本発明は、複数のコンピュータシステムが通信媒体により相互に接続されたコンピュータネットワーク間で暗号化した通信情報の送受信を行う電子通信装置において、

（ａ）公開鍵暗号方式を用い利用者相互の認証

（ｂ）公開鍵暗号方式を用い共通鍵の配布

（ｃ）前記共通鍵を用い通信情報の送受信

を命令するシステム本体部と、前記システム本体部の命令を実行するための暗号化処理と復号化処理を行う暗号処理部と、前記共通鍵を作成する鍵作成部とを具備することを特徴とする。

【００１７】また、一定時間及び一定通信回数ごとに利用者の一部が前記共通鍵を更新することのできる鍵作成トークンを持つ前記鍵作成部と、前記利用者の一部が通信を中止するとき、他の利用者に鍵作成トークンの使用を命令するシステム本体部とを具備することを特徴とする。さらに、サブグループ間の機密保持通信を行うために、サブグループ間に有効な共通鍵を作成する前記鍵作成部を具備することを特徴とする。

【００１８】

【作用】上記構成の電子通信装置によれば、あらかじめに公開鍵を利用者に配布し、通信情報を送信する利用者の秘密鍵を用いて公開暗号方式で暗号化することにより、この通信情報が前記送信する利用者か送信したことを保証し、さらにこの通信情報を受信する利用者の公開鍵を用いて暗号化することにより、この通信情報が受信人のみに解読でき、従来の装置にくらべ認証の際送信する通信情報が少なく相互認証を効率よく行うことができる。

4

【００１９】利用者は、相互認証後利用者間で、その後の通信の暗号に用いる共通鍵を共通鍵作成手段において作成し、前記公開暗号方式で配布することにより、安全に共通鍵を配布することができ、さらに定期的に更新することにより、通信の安全性を高めることができる。

【００２０】利用者が送信する通信情報は、送信を行う利用者の秘密鍵と前記公開暗号方式で配布された共通鍵の双方を用いて機密保持暗号化を行い、送信する通信情報が受信する利用者に関係なく同一のものとなり、同報機能の使用が可能になる。

【００２１】安全性向上のため、定期的に共通鍵の更新を行うが、利用者が勝手に更新を行うと共通鍵の一貫性を保持することができないため、鍵作成のプログラムの実行権である鍵作成トークンを使用可能な利用者に鍵の作成を委任することにより、共通鍵の一貫性を保持することが可能となる。

【００２２】鍵作成トークンを他の利用者に使用可能にすることにより、利用者は自由に通信に加入あるいは中止することが可能になる。利用者の一部でさらに機密保持通信を行うためのサブグループを作成する場合、複数の鍵作成トークンを用いてサブグループごとに異なった共通鍵を利用することにより、サブグループ内の通信においても機密保持が可能となる。

【００２３】

【実施例】以下、本発明の一実施例を図面を基に説明する。図1は本発明の一実施例の構成図である。ここではまず、図1を用いて利用者Ａと利用者Ｂが認証しあう手順を簡単に説明する。

【００２４】本電子通信装置は、通信媒体1を介して、複数のコンピュータシステム２、３、４、５が接続されている。利用者Ａは、コンピュータシステム２の入出力部２０に、利用者が利用者Ａであることを示す利用者Ａのパスワードを入力する。

【００２５】入出力部２０は、入力された利用者が利用者Ａであることを示す利用者Ａのパスワードをシステム本体部２１に送る。システム本体部２１は、入力された利用者が利用者Ａであることを示す利用者Ａのパスワードを暗号処理部２２に送る。

【００２６】システム本体部２１は、あらかじめ鍵管理データベース２３に登録されている利用者Ｂの公開鍵と利用者Ａの秘密鍵を暗号処理部２２に送り、暗号化を命令する。

【００２７】暗号処理部２２は、利用者Ｂの公開鍵を用いて、利用者Ａのパスワードを暗号化する。暗号処理部２２は、利用者Ａの秘密鍵を用い暗号化されたパスワードをさらに暗号化する。

【００２８】暗号処理部２２は、さらに暗号化された利用者Ａのパスワードをシステム本体部２１に送る。システム本体部２１は、このさらに暗号化された利用者Ａの

5

パスワードを通信制御部２４に送り、コンピュータシステム3 への送信を命令する。

【００２９】通信制御部２４は、さらに暗号化された利用者Ａのパスワード３０２を通信媒体1 を介してコンピュータシステム3 の通信制御部３４に送る。通信制御部３４は、通信媒体1 を介し通信制御部２４が送信したさらに暗号化された利用者Ａのパスワード３０２を受信する。

【００３０】通信制御部３４は、さらに暗号化された利用者Ａのパスワードをシステム本体部３１に送る。システム本体部３１は、このさらに暗号化された利用者Ａのパスワードを暗号処理部３２に送る。

【００３１】システム本体部３１は、鍵管理データベース３３に登録されている利用者Ａの公開鍵と利用者Ｂの秘密鍵を暗号処理部２２に送り、復号化を命令する。暗号処理部３２は、利用者Ａの公開鍵で、さらに暗号化された利用者Ａのパスワードを復号する。ここでは、さらに暗号化された利用者Ａのパスワードは、復号化された利用者Ａのパスワードになる。

【００３２】暗号処理部３２は、復号化された利用者Ａのパスワードをシステム本体部３１に送る。システム本体部３１は、正しく復号できたかを判断する。

【００３３】システム本体部３１は、復号できなかった場合、本装置を終了させる。システム本体部３１は、正しく復号できた場合、暗号処理部３２に復号化を命令する。

【００３４】暗号処理部３２は、利用者Ｂの秘密鍵で、復号化された利用者Ａのパスワードを復号する。暗号処理部３２は、さらに復号化された利用者Ａのパスワードをシステム本体部３１に送る。

【００３５】システム本体部３１は、正しく復号できたかを判断する。システム本体部３１は、復号できなかった場合、本装置を終了させる。なお、正しく復号できた場合、このさらに復号化された利用者Ａのパスワードは、利用者Ａのパスワードと同じものである。

【００３６】システム本体部３１は、正しく復号できた場合、さらに復号化された利用者Ａのパスワードを入出力部３０に送る。入出力部３０は、さらに復号化された利用者Ａのパスワード、つまり、利用者Ａのパスワードを出力する。

【００３７】利用者Ｂは、入出力部３０にさらに復号化された利用者Ａのパスワード、つまり、利用者Ａのパスワードが出力されたことにより、送信者が利用者Ａであることを認証する。

【００３８】この後、逆に利用者Ｂから利用者Ａに同様の手続きで送信することにより、利用者Ａと利用者Ｂの相互の認証を行う。以下、上述の利用者Ａと利用者Ｂの認証の手順を図2 のフローチャートと図3 の通信情報の形式を示す図を基に詳しく説明する。

【００３９】利用者Ａは、図2 に示す「Ａのパスワードを入力」２００のステップで、図1 のコンピュータシステム2 の入出力部２０に、図3 に示す利用者が利用者Ａであることを示す利用者Ａのパスワード３００を入力する。

6

【００４０】入出力部２０は、入力された利用者が利用者Ａであることを示す利用者Ａのパスワード３００をシステム本体部２１に送る。システム本体部２１は、入力された利用者が利用者Ａであることを示す利用者Ａのパスワード３００を暗号処理部２２に送る。

【００４１】システム本体部２１は、あらかじめされている鍵管理データベース２３に登録されている利用者Ｂの公開鍵と利用者Ａの秘密鍵を暗号処理部２２に送り、暗号化を命令する。

【００４２】暗号処理部２２は、ステップ「Ｂの公開鍵で暗号化」２０１にあるように、利用者Ｂの公開鍵を用いて、利用者Ａのパスワード３００を暗号化する。ここでは、利用者Ａのパスワード３００は、暗号化された利用者Ａのパスワード３０１になる。

【００４３】暗号処理部２２は、ステップ「Ａの秘密鍵で暗号化」２０２にあるように、利用者Ａの秘密鍵を用いて、暗号化された利用者Ａのパスワード３０１を暗号化する。ここでは、暗号化された利用者Ａのパスワード３０１は、さらに暗号化された利用者Ａのパスワード３０２になる。

【００４４】暗号処理部２２は、さらに暗号化された利用者Ａのパスワード３０２をシステム本体部２１に送る。システム本体部２１は、このさらに暗号化された利用者Ａのパスワード３０２を通信制御部２４に送り、コンピュータシステム3 への送信を命令する。

【００４５】通信制御部２４は、ステップ「暗号化されたパスワードの送信」２０３にあるように、さらに暗号化された利用者Ａのパスワード３０２を通信媒体1 を介してコンピュータシステム3 の通信制御部３４に送る。

【００４６】通信制御部３４は、ステップ「暗号化されたパスワードの受信」２０４にあるように、通信媒体1 を介し通信制御部２４が送信したさらに暗号化された利用者Ａのパスワード３０２を受信する。

【００４７】通信制御部３４は、さらに暗号化された利用者Ａのパスワード３０２をシステム本体部３１に送る。システム本体部３１は、このさらに暗号化された利用者Ａのパスワード３０２を暗号処理部３２に送る。

【００４８】システム本体部３１は、鍵管理データベース３３に登録されている利用者Ａの公開鍵と利用者Ｂの秘密鍵を暗号処理部２２に送り、復号化を命令する。暗号処理部３２は、ステップ「Ａの公開鍵で復号化」２０５にあるように、利用者Ａの公開鍵で、さらに暗号化された利用者Ａのパスワード３０２を復号する。ここでは、さらに暗号化された利用者Ａのパスワード３０２は、復号化された利用者Ａのパスワード３０３になる。

【００４９】暗号処理部３２は、復号化された利用者Ａ

7

のパスワード３０３をシステム本体部３１に送る。システム本体部３１は、ステップ「 復号できた？」２０６にあるように正しく復号できたかを判断する。

【００５０】システム本体部３１は、復号できなかった場合、ステップ「 エラー終了」２０７にあるように、本装置を終了させる。なお、正しく復号できた場合、この復号化された利用者Ａのパスワード３０３は、暗号化された利用者Ａのパスワード３０１と同じものになる。

【００５１】システム本体部３１は、正しく復号できた場合、暗号処理部３２に復号化を命令する。暗号処理部３２は、ステップ「 Ｂの秘密鍵で復号化」２０８にあるように、利用者Ｂの秘密鍵で、復号化された利用者Ａのパスワード３０３を復号する。ここでは、復号化された利用者Ａのパスワード３０３は、さらに復号化された利用者Ａのパスワード３０４になる。

【００５２】暗号処理部３２は、さらに復号化された利用者Ａのパスワード３０４をシステム本体部３１に送る。システム本体部３１は、ステップ「 復号できた？」２０９にあるように、正しく復号できたかを判断する。

【００５３】システム本体部３１は、復号できなかった場合、ステップ「 エラー終了」２０７にあるように、本装置を終了させる。なお、正しく復号できた場合、このさらに復号化された利用者Ａのパスワード３０４は、利用者Ａのパスワード３００と同じものになる。

【００５４】システム本体部３１は、正しく復号できた場合、さらに復号化された利用者Ａのパスワード３０４、つまり、利用者Ａのパスワード３００を入出力部３０に送る。

【００５５】入出力部３０は、ステップ「 Ａのパスワードの出力」２１０にあるように、さらに復号化された利用者Ａのパスワード３０４、つまり、利用者Ａのパスワード３００を出力する。

【００５６】利用者Ｂは、入出力部３０にさらに復号化された利用者Ａのパスワード３０４、つまり、利用者Ａのパスワード３００が出力されたことにより、送信者が利用者Ａであることを認証する。

【００５７】利用者全員が暗号化処理のためにもつ共通鍵を配布する手順は、共通鍵を持つ利用者あるいは、共通鍵を作成した利用者が、上述のパスワードを送信する手順で、パスワードではなく共通鍵を通信情報として送信することにより配布する。

【００５８】また、パスワードと共通鍵を同時に送信することにより、認証と共通鍵の配布が一度に行うことができる。本電子通信装置の機密保持暗号化通信の手順を、図1の構成図を基に簡単に説明する。

【００５９】利用者Ａは、入出力部２０に利用者Ａの通信情報を入力する。入出力部２０は、利用者Ａの通信情報をシステム本体部２１に送る。システム本体部２１は、利用者Ａの通信情報を暗号処理部２２に送る。

【００６０】システム本体部２１は、鍵管理データベース２３に登録されている利用者Ａの秘密鍵と共通鍵を暗号処理部２２に送り、暗号化を命令する。暗号処理部２２は、利用者Ａの通信情報を利用者Ａの秘密鍵を用いて暗号化する。

【００６１】暗号処理部２２は、暗号化された利用者Ａの通信情報を鍵管理データベース２３に登録されている共通鍵を用いてさらに暗号化する。暗号処理部２２は、さらに暗号化された利用者Ａの通信情報をシステム本体部２１に送る。

【００６２】システム本体部２１は、さらに暗号化された利用者Ａの通信情報を通信制御部２４に送り、コンピュータシステム３、４、５に送信を命令する。通信制御部２４は、通信媒体1を介して、さらに暗号化された利用者Ａの通信情報を利用者Ｂ、利用者Ｃ、利用者Ｄのコンピュータシステム３、４、５の通信制御部３４、４４、５４に送信する。

【００６３】コンピュータシステム３、４、５の通信制御部３４、４４、５４は、さらに暗号化された利用者Ａの通信情報を受信する。通信制御部３４、４４、５４は、さらに暗号化された利用者Ａの通信情報を本体システム部３１、４１、５１に送る。

【００６４】本体システム部３１、４１、５１は、さらに暗号化された利用者Ａの通信情報を暗号処理部３２、４２、５２に送る。本体システム部３１、４１、５１は、鍵管理データベース３３、４３、５３に登録されている共通鍵と利用者Ａの公開鍵を暗号処理部３２、４２、５２に送り、復号化を命令する。

【００６５】暗号処理部３２、４２、５２は、さらに暗号化された利用者Ａの通信情報を、共通鍵で復号する。暗号処理部３２、４２、５２は、復号化された利用者Ａの通信情報を本体システム部３１、４１、５１に送る。

【００６６】本体システム部３１、４１、５１は、正しく復号できたかを判断する。本体システム部３１、４１、５１は、復号できなかった場合は、本装置を終了させる。

【００６７】本体システム部３１、４１、５１は、復号化された利用者Ａの通信情報の復号化を暗号処理部３２、４２、５２に命令する。暗号処理部３２、４２、５２は、利用者Ａの公開鍵で復号化された利用者Ａの通信情報を復号する。

【００６８】暗号処理部３２、４２、５２は、このさらに復号化された利用者Ａの通信情報を本体システム部３１、４１、５１に送る。本体システム部３１、４１、５１は、正しく復号できたかを判断する。本体システム部３１、４１、５１は、復号できなかった場合は、本装置を終了させる。

【００６９】本体システム部３１、４１、５１は、正しく復号できた場合、このさらに復号化された利用者Ａの通信情報、つまり、利用者Ａの通信情報を入出力部３０、４０、５０に送り、出力を命令する。

9

【００７０】入出力部３０、４０、５０は、さらに復号化された利用者Ａの通信情報、つまり、利用者Ａの通信情報を出力する。以下、上述した通信情報の機密保持暗号化通信を具体的に、図4 のフローチャートと図5 の通信情報の形式を示す図を基に説明する。

【００７１】利用者Ａは、図4 のステップ「 Ａの通信情報入力」４００にあるように、図1 の入出力部２０に図５に示す利用者Ａの通信情報５００を入力する。入出力部２０は、利用者Ａの通信情報５００をシステム本体部２１に送る。

【００７２】システム本体部２１は、利用者Ａの通信情報５００を暗号処理部２２に送る。システム本体部２１は、鍵管理データベース２３に登録されている利用者Ａの秘密鍵と共通鍵を暗号処理部２２に送り、暗号化を命令する。

【００７３】暗号処理部２２は、ステップ「 Ａの秘密鍵で暗号化」４０１にあるように、利用者Ａの通信情報５００を利用者Ａの秘密鍵を用いて暗号化する。ここでは、利用者Ａの通信情報５００は、暗号化された利用者Ａの通信情報５０１になる。

【００７４】なお、この暗号化は秘密鍵を有する真の利用者しか行えないため、通信情報に署名を行うことと同様の効果がある。暗号処理部２２は、ステップ「 共通鍵で暗号化」４０２にあるように、暗号化された利用者Ａの通信情報５０１を、鍵管理データベース２３に登録されている共通鍵を用いて暗号化する。ここでは、暗号化された利用者Ａの通信情報５０１は、さらに暗号化された利用者Ａの通信情報５０２になる。

【００７５】暗号処理部２２は、さらに暗号化された利用者Ａの通信情報５０２をシステム本体部２１に送る。システム本体部２１は、さらに暗号化された利用者Ａの通信情報５０２を通信制御部２４に送り、コンピュータシステム３、４、５に送信を命令する。

【００７６】通信制御部２４は、ステップ「 通信情報の送信」４０３にあるように、通信媒体1 を介して、さらに暗号化された利用者Ａの通信情報５０２を利用者Ｂ、利用者Ｃ、利用者Ｄのコンピュータシステム３、４、５の通信制御部３４、４４、５４に送信する。

【００７７】コンピュータシステム３、４、５の通信制御部３４、４４、５４は、ステップ「 通信情報の受信」４０４にあるように、さらに暗号化された利用者Ａの通信情報５０２を受信する。

【００７８】通信制御部３４、４４、５４は、さらに暗号化された利用者Ａの通信情報５０２を本体システム部３１、４１、５１に送る。本体システム部３１、４１、５１は、さらに暗号化された利用者Ａの通信情報５０２を暗号処理部３２、４２、５２に送る。

【００７９】本体システム部３１、４１、５１は、鍵管理データベース３３、４３、５３に登録されている共通鍵と利用者Ａの公開鍵を暗号処理部３２、４２、５２に送り、復号化を命令する。

10

【００８０】暗号処理部３２、４２、５２は、ステップ「 共通鍵で復号化」４０５にあるように、さらに暗号化された利用者Ａの通信情報５０２を、共通鍵で復号する。ここでは、さらに暗号化された利用者Ａの通信情報５０２は、復号化された利用者Ａの通信情報５０３になる。

【００８１】暗号処理部３２、４２、５２は、復号化された利用者Ａの通信情報５０３を本体システム部３１、４１、５１に送る。本体システム部３１、４１、５１は、ステップ「 復号できた？」４０６にあるように、正しく復号できたかを判断する。

【００８２】本体システム部３１、４１、５１は、復号できなかった場合は、ステップ「 エラー終了」４０７にあるように、本装置を終了させる。なお、正しく復号できた場合、この復号化された利用者Ａの通信情報５０３は、暗号化された利用者Ａの通信情報５０１と同じものになる。

【００８３】本体システム部３１、４１、５１は、復号化された利用者Ａの通信情報５０３の復号化を暗号処理部３２、４２、５２に命令する。暗号処理部３２、４２、５２は、ステップ「 Ａの公開鍵で復号化」４０８にあるように、利用者Ａの公開鍵で復号化された利用者Ａの通信情報５０３を復号する。ここでは、復号化された利用者Ａの通信情報５０３は、さらに復号化された利用者Ａの通信情報５０４になる。

【００８４】暗号処理部３２、４２、５２は、このさらに復号化された利用者Ａの通信情報５０４を本体システム部３１、４１、５１に送る。本体システム部３１、４１、５１は、ステップ「 復号できた？」４０９にあるように、正しく復号できたかを判断する。本体システム部３１、４１、５１は、復号できなかった場合は、ステップ「 エラー終了」４０７にあるように、本装置を終了させる。

【００８５】なお、正しく復号できた場合、このさらに復号化された利用者Ａの通信情報５０４は、利用者Ａの通信情報５００と同じものになる。。本体システム部３１、４１、５１は、正しく復号できた場合、このさらに復号化された利用者Ａの通信情報５０４、つまり、利用者Ａの通信情報５００を入出力部３０、４０、５０に送り、出力を命令する。

【００８６】入出力部３０、４０、５０は、ステップ「 通信情報の出力」４１０にあるように、さらに復号化された利用者Ａの通信情報５０４、つまり、利用者Ａの通信情報５００を出力する。

【００８７】安全性を確保するため、共通鍵を更新する例を図6 のフローチャートを基に説明する。共通鍵の更新は、上述した機密保持暗号化通信において、鍵管理データベース２３に登録されている共通鍵を用いて暗号化するとき（ 図4 のフローチャートのステップ「 共通鍵で

11

暗号化」４０２の処理）に行う。ここでは、利用者Ａが鍵作成部に共通鍵を作成するプログラムの実行権である共通鍵作成トークンを持ち、利用者Ａが一定回数ごとに通信を行うと、共通鍵を更新作成するものとする。

【００８８】本体システム部２１は、ステップ「共通鍵作成トークンの有無？」６００にあるように鍵作成部２５に共通鍵作成トークンがあるか否か判断する。共通鍵作成トークンが無い場合、つまり、利用者Ａ以外の利用者が共通鍵を用いて通信情報を暗号化する場合、ステップ「今までの共通鍵で暗号化」６０１にあるように、本体システム部２１は、現在使われている共通鍵での暗号化を命令（上述の図4のフローチャートのステップ「共通鍵で暗号化」４０２の処理）し、機密保持暗号化通信を行う。

【００８９】共通鍵作成トークンを持つ場合、つまり、利用者Ａが共通鍵を用いて通信情報を暗号化する場合、本体システム部２１は、ステップ「カウンタを＋１」６０２にあるように、鍵管理データベース２３にあるカウンタを更新する。

【００９０】本体システム部２１は、ステップ「カウンタが設定値以上？」６０３にあるように、カウンタが設定値以上かどうか判断する。カウンタが、設定値未満の場合、ステップ「今までの共通鍵で暗号化」６０１にあるように、本体システム部２１は、現在使われている共通鍵での暗号化を命令（上述の図4のフローチャートのステップ「共通鍵で暗号化」４０２の処理）し、機密保持暗号化通信を行う。

【００９１】設定値に達した場合、本体システム部２１は、ステップ「共通鍵を作成」６０４にあるように、新しい共通鍵を作成することを鍵作成部２５に命令する。鍵作成部２５は、新しい共通鍵を作成し、ステップ「共通鍵を登録」６０５にあるように、鍵管理データベース２３に登録する。

【００９２】本体システム部２１は、ステップ「カウンタを０」６０６にあるように、鍵管理データベース２３のカウンタを０にする。本体システム部２１は、鍵管理データベース２３に登録した新しい共通鍵を暗号処理部２２に送り、暗号化の処理を命令する。

【００９３】暗号処理部２２は、上述の認証の手順つまり、共通鍵配布の手順で暗号化の処理をし、本体システム部２１に送る。本体システム部２１は、この暗号化の処理をされた共通鍵を通信制御部２４に送る。

【００９４】通信制御部２４は、ステップ「共通鍵の配布」６０７にあるように、上述の認証の手順つまり、共通鍵配布の手順で他の利用者全員に配布する。利用者Ａ、Ｂ、Ｃ、Ｄのコンピュータシステム２、３、４、５は、ステップ「新しい共通鍵で暗号化」６０８にあるように、この新しい共通鍵で通信情報を暗号化（上述の図4のフローチャートの「共通鍵で暗号化」４０２の処理）し、機密保持暗号化通信を行う。

12

【００９５】このように定期的に共通鍵を更新することにより、万が一、共通鍵が漏洩した場合でも通信の安全性を保持することができる。共通鍵作成トークンを持つ利用者が、他の利用者に共通鍵作成トークンを移す共通鍵作成トークンの委譲処理について説明する。

【００９６】通常の通信において、共通鍵作成トークンの委譲は共通鍵の一貫性の保持と、一定回数ごとの共通鍵の更新ということを考慮すると避けるべきことである。しかし、共通鍵作成トークンを持つ者が通信を中止する場合、一定回数及び一定時間ごとの共通鍵の更新ができなくなるため、他のメンバに対して共通鍵作成トークンを委譲する必要がある。

【００９７】委譲処理は、上述の認証の手順、つまり、共通鍵配布の手順と同様の通信手順で、共通鍵作成トークンの委譲の命令を通信情報として送信することで行う。具体的に、図7のフローチャートを基に、利用者Ａが通信を中止し、利用者Ａが共通鍵作成トークンを持つ場合には共通鍵作成トークンをＢに委譲処理する手順を説明する。

【００９８】利用者Ａは、ステップ「通信中止コマンド入力」７００にあるように、入出力部２１に通信を中止するコマンドを入力する。入出力部２１は、暗号処理部２２に通信中止の命令を送る。

【００９９】暗号処理部２２は、ステップ「共通鍵作成トークンの有無？」７０１にあるように、鍵管理データベース２３に共通鍵作成トークンがあるか否かを判断する。共通鍵作成トークンが無い場合、暗号処理部２２は、通信制御部２４に通信を中止し、通信媒体1との接続を解除する命令を送る。

【０１００】通信制御部２４は、ステップ「接続解除」７０２にあるように、コンピュータシステム2と通信媒体1との接続を解除する。共通鍵作成トークンがある場合、暗号処理部２２は、入出力部２１に共通鍵作成トークンを委譲する利用者名の入力を促す提示を行わせる。

【０１０１】利用者Ａは、ステップ「委譲する利用者名の入力」７０３にあるように、どの利用者に共通鍵作成トークンを委譲するかの入力を入出力部２１に行う。入出力部２１は、共通鍵作成トークンの委譲の命令を暗号処理部２２に送る。

【０１０２】暗号処理部２２は、通信制御部２４に共通鍵作成トークンの委譲の命令を送る。通信制御部２４は、ステップ「共通鍵作成トークンの委譲命令の送信」７０４にあるように、上述の認証の手順、つまり、共通鍵配布の手順と同様の通信手順で、共通鍵作成トークンの委譲の命令を利用者Ｂのコンピュータシステム3の通信制御部３４に送信する。

【０１０３】通信制御部３４は、ステップ「共通鍵作成トークンの委譲命令の受信」７０５にあるように、利用者Ａの共通鍵作成トークンの委譲命令を受信し、暗号処理部３２に送る。

13

【０１０４】暗号処理部３２は、ステップ「 共通鍵作成トークンの登録」７０６にあるように、利用者Ａの共通鍵作成トークンの委譲命令を解読し、今後共通鍵作成トークンを持つことを鍵管理データベース３３に登録する。

【０１０５】暗号処理部３２は、共通鍵作成トークンの登録が完了したことを通信制御部３４に送る。通信制御部３４は、ステップ「 登録完了メッセージの送信」７０７にあるように、共通鍵作成トークンの登録が完了したことを示すメッセージを利用者Ａのコンピュータシステム２の通信制御部２４に送信する。

【０１０６】通信制御部２４は、ステップ「 登録完了メッセージの受信」７０８にあるように、共通鍵作成トークンの登録が完了したことを示すメッセージを受信。通信制御部２４は、暗号処理部２２に共通鍵作成トークンの登録が完了したことを示すメッセージを送る。

【０１０７】暗号処理部２２は、共通鍵作成トークンの登録が完了したことを示すメッセージを解読し、通信を中止し、通信媒体1との接続を解除する命令を通信制御部２４に送る。

【０１０８】通信制御部２４は、ステップ「 接続解除」７０２にあるように、コンピュータシステム２と通信媒体1との接続を解除する。このように、共通鍵作成トークンの委譲により、通信の自由な参加、退席が可能になる。

【０１０９】通信中に利用者の一部分で、さらに機密保持通信を行いたい場合のサブグループ作成の手順について、図8のフローチャートと図9のサブグループを管理するためのグループ管理情報群の構造を示す図を基に説明する。ここでは、グループ名、利用者情報リスト、鍵作成トークンの有無、共通鍵、カウンタという横一列がひとつのグループ管理情報である。

【０１１０】利用者Ａは、図8に示すステップ「 グループ情報入力」８００にあるように、入出力部２１にサブグループの名称であるグループ名、利用者名や利用者のアドレス、共通鍵作成トークンの有無の入力を行う。ここでは、入出力部２１は、グループ管理部２６に入力されたグループ名、利用者情報（メンバ名、アドレス）、共通鍵作成トークンの有無をグループ管理部２６に送る。

【０１１１】グループ管理部２６は、ステップ「 グループ情報登録」８０１にあるように、図9に示すグループ管理情報９０に、グループ名をグループ名９００のように登録し、利用者情報を利用者情報リスト９０１、９０２、９０３のように登録し、共通鍵作成トークンの有無を共通鍵作成トークンの有無９０４のように登録する。ここでは、「 有」と登録する。

【０１１２】グループ管理部２６は、鍵作成部２５に共通鍵の作成を命令する。鍵作成部２５は、ステップ「 共通鍵の作成」８０２にあるように、サブグループ内の共通鍵を作成する。

14

【０１１３】鍵作成部２５は、作成したサブグループ内の共通鍵をグループ管理部２６に送る。グループ管理部２６は、ステップ「 共通鍵の登録」８０３にあるように、グループ管理情報９０に、サブグループ内の共通鍵をサブグループ共通鍵９０５のように、グループ管理情報９０に登録する。

【０１１４】グループ管理部２６は、ステップ「 カウンタを０」８０４にあるように、サブグループ内の共通鍵の更新のため、サブグループ内の共通鍵の使用回数を数えるためのグループ通信カウンタ９０６を０にセットする。

【０１１５】グループ管理部２６は、グループ管理情報９０の共通鍵作成トークンの有無９０４を「 無」としたグループ管理情報を暗号処理部２２に送る。暗号処理部２２は、サブグループの利用者のみに、ステップ「 グループ情報の配布」８０５にあるように、前記グループ管理情報を上述の認証の手順つまり、共通鍵配布と同様の手順で配布する。

【０１１６】配布された前記グループ管理情報のサブグループ共通鍵を利用することにより、前記グループ情報管理を持つサブグループの利用者間のみで、秘密情報通信が可能となる。

【０１１７】

【発明の効果】本発明の電子通信装置によれば、相互認証の際、利用者はあらかじめ配布された公開鍵を持ち、通信情報を送信する利用者の秘密鍵を用いて公開暗号化方式で暗号化することにより、前記通信情報が前記利用者から送信されたことを保証し、さらに前記通信情報を受信人の公開鍵を用いて暗号化することにより、通信情報が受信人のみに解読でき、従来の装置にくらべ認証の際送信する通信情報が少なく相互認証を効率よく行うことができる。

【０１１８】鍵作成トークンを持つ利用者が共通鍵を作成し、上述の公開暗号方式で配布することにより、安全に共通鍵を配布することができ、さらに定期的に更新することにより、通信の安全性を高めることができる。

【０１１９】また、複数の利用者の通信において、発信人の秘密鍵と公開暗号方式で配布された共通鍵の双方を用いて暗号化を行った場合、同一の通信情報の送信で共通鍵を持つ利用者のみ受信が可能である。

【図面の簡単な説明】

【図1】本発明の一実施例の構成を示す図。

【図2】本発明の一実施例における利用者の認証の手順を示す図。

【図3】本発明の一実施例における利用者の認証の際に暗号化された通信情報の形式と復号化された通信情報の形式をを示す図。

【図4】本発明の一実施例における機密暗号化通信の手順を示す図。

15

【 図5 】本発明の一実施例における機密暗号化通信の際に暗号化された通信情報の形式と復号化された通信情報の形式をを示す図。

【 図6 】本発明の一実施例における共通鍵の更新の手順を示す図。

【 図7 】本発明の一実施例における共通鍵作成トークンの委譲処理の手順を示す図。

【 図8 】本発明の一実施例におけるサブグループの作成の手順を示す図。

【 図9 】本発明の一実施例におけるサブグループ作成の際のグループ管理情報群の構造を示す図。

【 符号の説明】

1　通信媒体

２、３、４、５　コンピュータシステム

２０、３０、４０、５０　入出力部

２１、３１、４１、５１　本体システム部

２２、３２、４２、５２　暗号処理部

２３、３３、４３、５３　鍵管理データベース

２４、３４、４４、５４　通信制御部

２５、３５、４５、５５　鍵作成部

２６、３６、４６、５６　グループ管理部

16

３００　利用者Ａが入力した通信情報

３０１　利用者Ｂの公開鍵で暗号化されたパスワードの形式

３０２　利用者Ａの秘密鍵で暗号化されたパスワードの形式

３０３　利用者Ａの公開鍵で復号化されたパスワードの形式

３０４　利用者Ｂの秘密鍵で復号化されたパスワードの形式

５００　利用者Ａが入力した通信情報の形式

５０１　利用者Ａの秘密鍵で暗号化された通信情報の形式

５０２　共通鍵で暗号化された通信情報の形式

５０３　共通鍵で復号化された通信情報の形式

５０４　Ａの公開鍵で復号化された通信情報の形式

９０　グループ管理情報

９００　グループ名

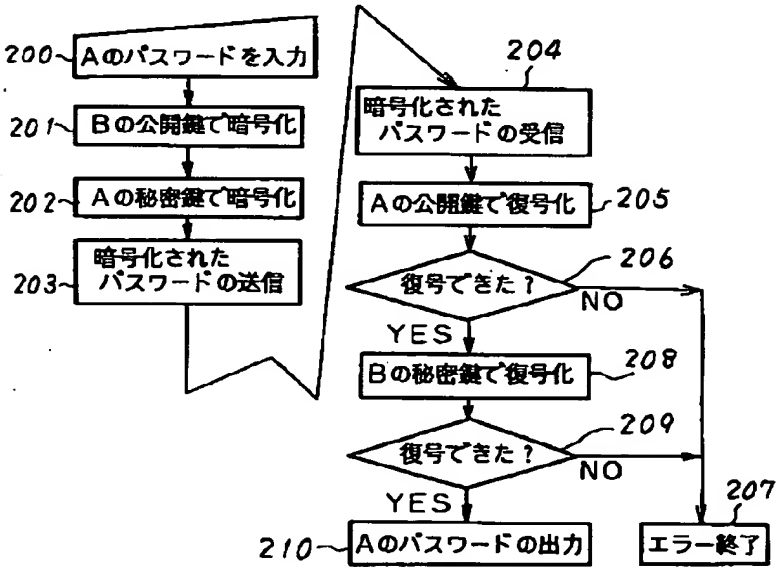
９０１、９０２、９０３　利用者情報リスト

９０４　鍵作成トークンの有無

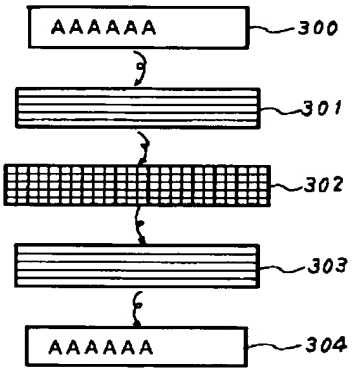
９０５　サブグループ共通鍵

９０６　グループ通信カウンタ

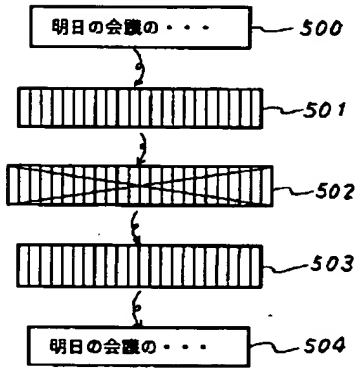
【 図2 】



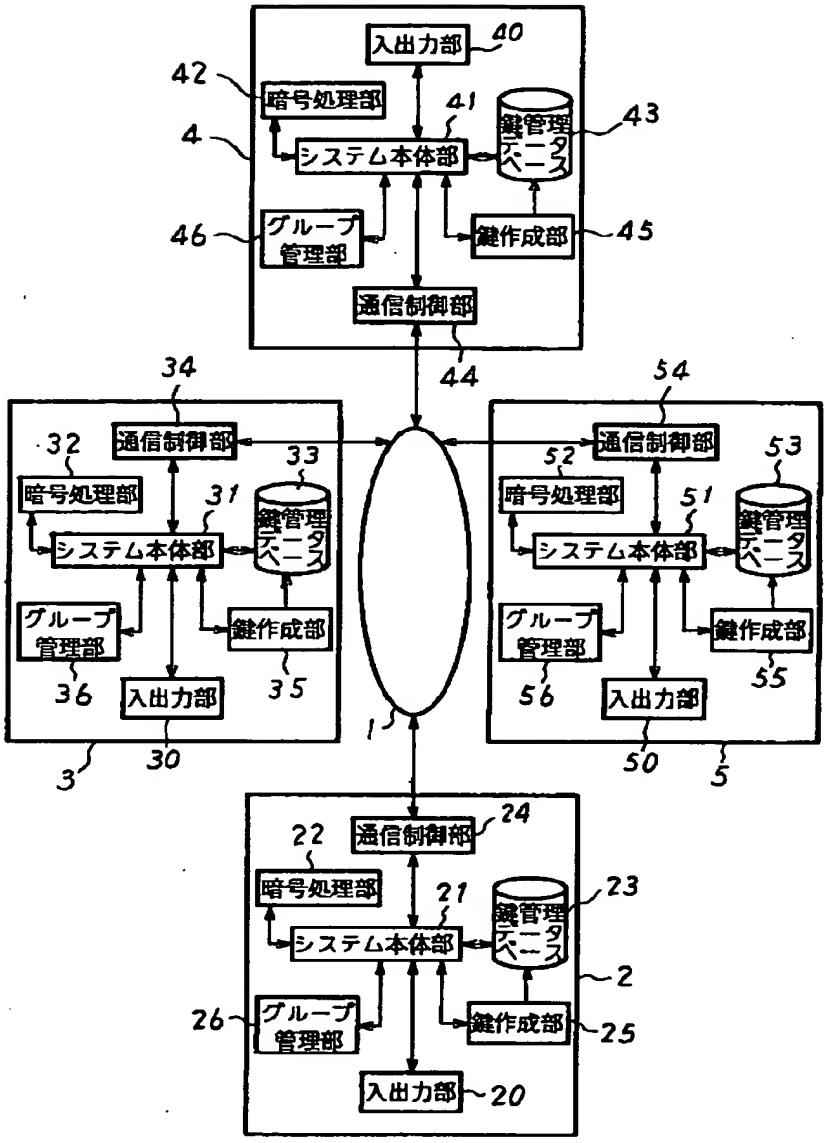
【 図3 】



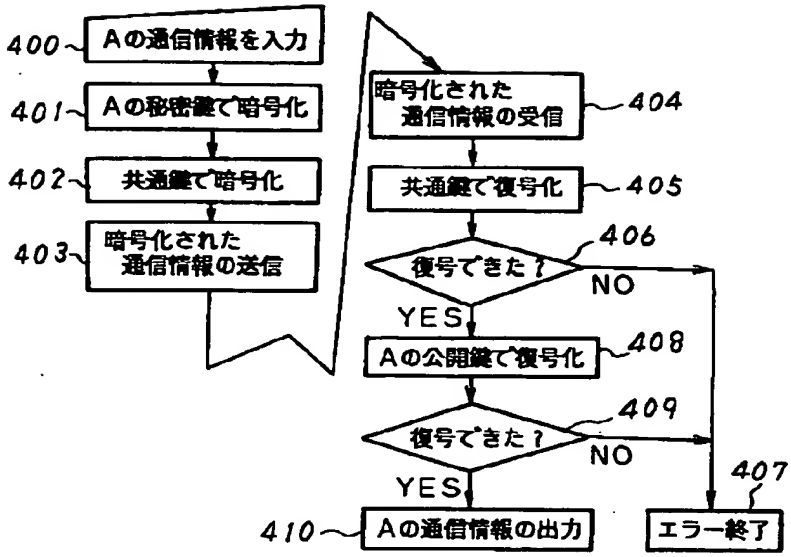
【 図5 】



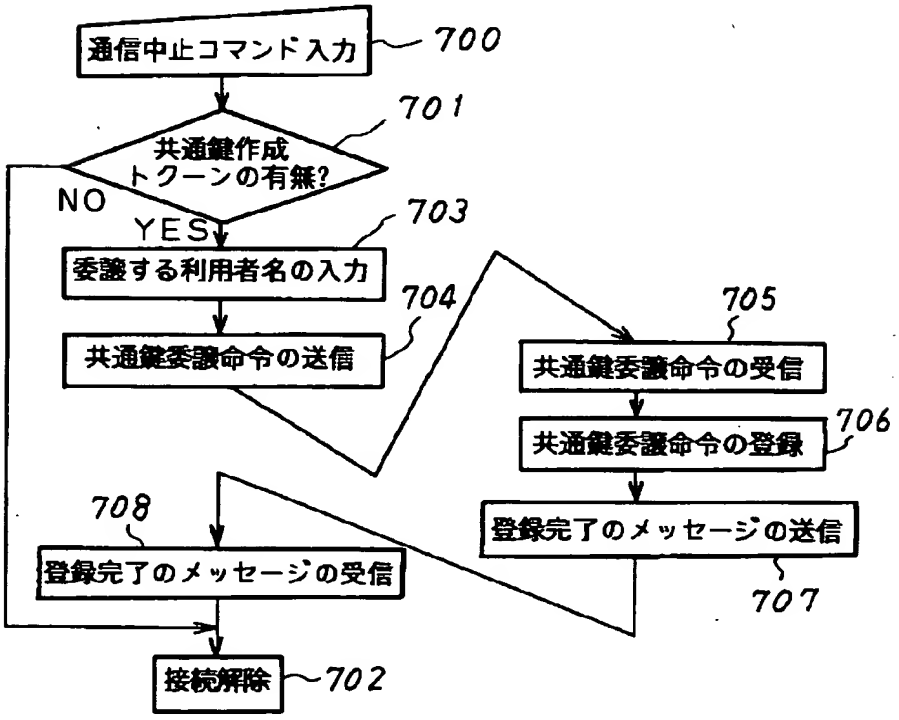
【 図1 】


入出力部
40
42
暗号処理部
41
鍵管理データベース
43
4
システム本体部
グループ管理部
46
鍵作成部
45
通信制御部
44
34
54
32
通信制御部
52
通信制御部
53
33
暗号処理部
31
暗号処理部
51
鍵管理データベース
システム本体部
システム本体部
鍵管理データベース
グループ管理部
鍵作成部
グループ管理部
鍵作成部
36
入出力部
35
56
入出力部
55
1
3
30
50
5
22
通信制御部
24
暗号処理部
21
鍵管理データベース
23
システム本体部
2
26
グループ管理部
鍵作成部
25
入出力部
20

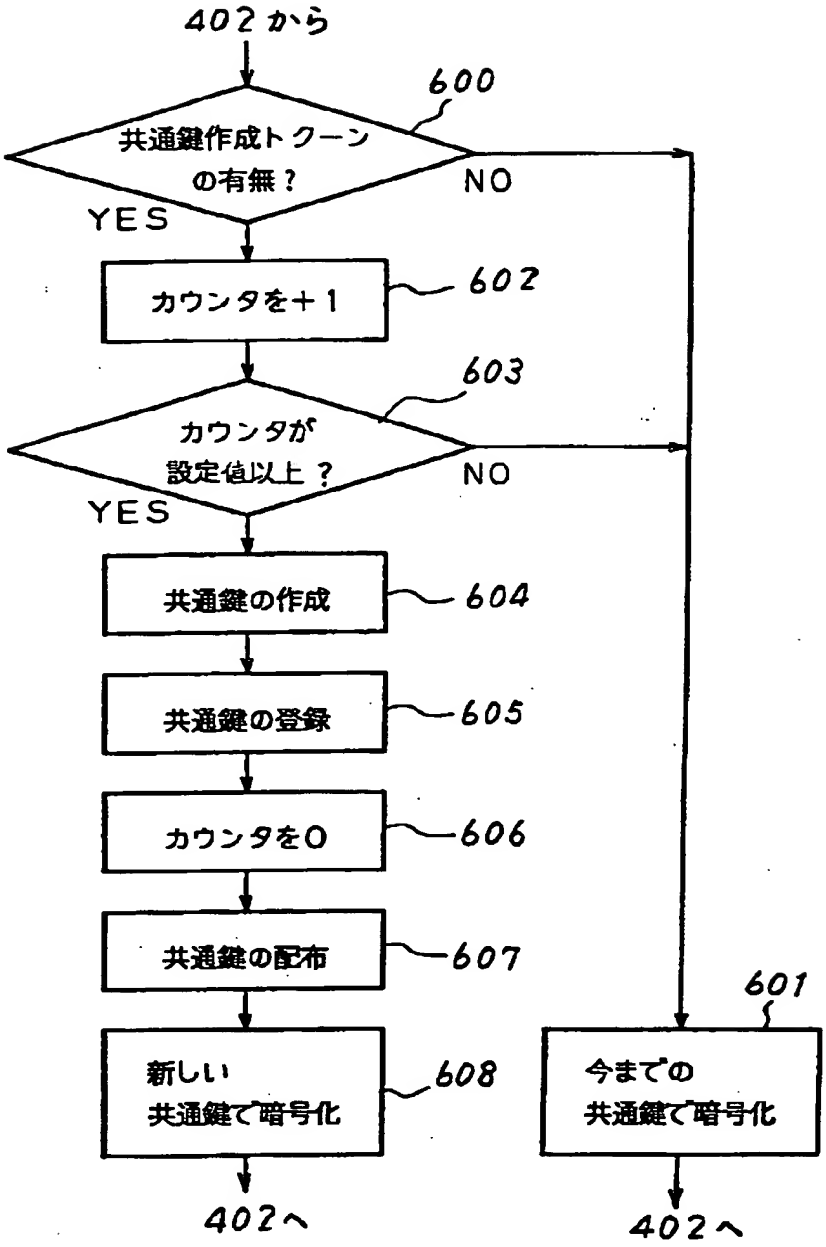
【 図4 】


400
Aの通信情報を入力
401
Aの秘密鍵で暗号化
402
共通鍵で暗号化
403
暗号化された
通信情報の送信
暗号化された
通信情報の受信
404
共通鍵で復号化
405
406
復号できた？
NO
YES
Aの公開鍵で復号化
408
409
復号できた？
NO
YES
407
410
Aの通信情報の出力
エラー終了

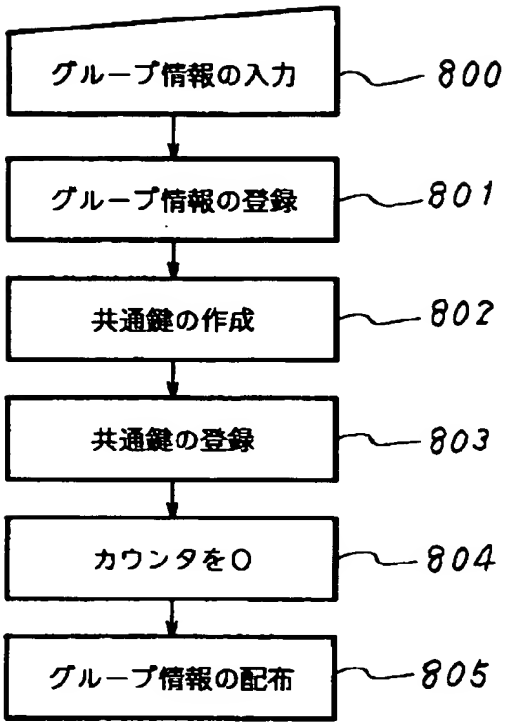
【 図7 】


通信中止コマンド入力
700
701
共通鍵作成
トクーンの有無?
NO
YES
703
委譲する利用者名の入力
704
共通鍵委譲命令の送信
705
共通鍵委譲命令の受信
706
共通鍵委譲命令の登録
登録完了のメッセージの送信
707
708
登録完了のメッセージの受信
接続解除
702

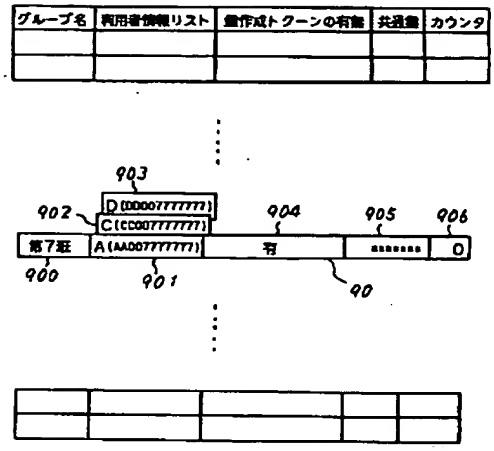
【 図6 】


402 から
600
共通鍵作成トクーンの有無？
NO
YES
602
カウンタを＋1
603
カウンタが設定値以上？
NO
YES
604
共通鍵の作成
605
共通鍵の登録
606
カウンタを0
607
共通鍵の配布
608
新しい共通鍵で暗号化
402へ
601
今までの共通鍵で暗号化
402へ

【 図8 】



【 図9 】



フロント ページの続き

(51)Int.Cl.[5]		識別記号	庁内整理番号	FI		技術表示箇所
G０６F	13/00	３５１　Z	7368－5B			
H０４L	9/06					
	9/14					
	12/22					
			8732－5K	H０４L	11/26	